View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by KnowledgeBank at OSU

Authenticity and Audit Trails

Maintaining an audit trail—the chronological record of activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities—is inextricably linked to the provenance of a record, not just at the point of appraisal and accessioning, but from the record's point of creation, through its primary and active use by an individual or within an organization, and throughout its archival life.[1] Archival theory developed from humans having the physical abilities to read and analyze information, which is linked to the media on which it was written, however as Stielow noted, "…this approach is no longer sufficient. Stare as you might, the floppy disk is indecipherable to the human eye…"[2] Hedstrom stated, that "On the most basic level, electronic records are not inert physical items; rather, they are dynamic, interactive documents that combine information from many different sources and several different formats into complex, virtual documents…The content of an electronic document is recorded separately from the software that organizes it into an intelligible, logical structure for transmission or viewing on a screen." [3] There is the need to authenticate the provenance—information regarding the origins, custody, and ownership of an item or collection—of the all items that are accessioned, regardless of format, albeit a more complex undertaking for electronic records. [4]

The international standard for records management, ISO 15489, suggests that authoritative records have the characteristics of: authenticity – an authentic record proves to be what it purports to be; reliability – a reliable record is one whose contents can be trusted as a full and accurate; integrity – referring to a record being complete and unaltered; and useability – a usable record is one which can be located, retrieved, presented and interpreted.[5] As logical, not physical entities, it may be harder to establish the authenticity, reliability, and integrity of electronic records. However, electronic recordkeeping systems and trusted digital repositories

that capture audit trails should be able to provide evidence of authenticity over time, document the reliability and integrity of the records, and assist in their useability.

A key incentive for developing more systematic audit mechanisms to establish and certify authenticity, is the fact that archivists are unlikely to be working with original archival electronic materials. All archival electronic records may be more accurately thought of as copies of original records—preservation copies made according to the particular standards, and use copies that may be generated according to user needs.[6] An audit trail for electronic records and digital objects, consists of the "documentation of all the interactions with records within an electronic system in which any access to the system is recorded as it occurs."[7] [8] Whether approaching the topic from a records management or an archival point of view, the audit process and trail assists in establishing not only the authenticity, integrity, reliability and useability of records, but documents the handling and transformations during preservation activities.

If archivists are able to identify potential electronic recordkeeping systems, influence the technical standards for such systems and ultimately capture the type of documentation necessary to facilitate the future use of records created by these systems, then it is likely that electronic records of historical value can later be transferred to archival custody more effectively with some of the cost of processing, arrangement and preservation already paid. While these types of cost benefits have not yet been fully realized—in part due to systems that are not designed with archival input, or with the need to provide for authentic, reliable, usable records with integrity beyond the systems lifecycle—the profession and its allied partners have been developing national and international standards to that end.

The Advent of Electronic Recordkeeping Standards

Prior to the advent of the aforementioned ISO standard, Bearman and Sochats' Pittsburgh Project laid out a foundation for functional recordkeeping requirements. They suggested, "Any organization that wants to use electronic documentation as evidence in the future will need to satisfy the requirements of evidence [audit trails] in the normal course of conducting its business." [9] Simultaneous to the Pittsburgh project, Luciana Duranti, et al, collaborated with the U.S. Department of Defense (DoD) to transform theoretical electronic records authenticity hypotheses into implementable and assessable functional requirements for systems that generate electronic records.[10] The project led to the establishment in 1997 of the DoD 5015.2 -STD: Design Criteria Standard for Electronic Records Management Software Applications, as well as to the InterPARES Project in 1999.

DoD 5015.2-STD (originally adopted in 1997, revised in 2002 and 2007 and reissued in 2015) established a set of criteria from which a records management software application can be certified[11]. Developed as a standard for the DoD, as early as 1998 it was endorsed by the U.S. National Archives and Records Administration, and it has become a de facto standard in the United States.[12] Of the nineteen major mandatory requirements, two pertain to the need for and management of audit trails—C.2.2.9 System Audits and C.2.2.11 System Management Requirements.[13]

The first phase of InterPARES (1999–2001) focused on establishing requirements for authenticity of inactive records generated and maintained in large databases and document management systems created by government agencies[14]. It established audit trail related benchmark criteria that an institution should maintain to demonstrate that it has: defined, implemented and monitors access privileges for all interactions with records (A.2); developed procedures to prevent and correct loss or corruption of records (A.3); and developed procedures

for the transfer of records to a preservation environment(A.8). Further, it established baseline requirements that support the production of authentic copies of electronic records. B.2 requires that "…the activity of reproduction has been documented…" i.e. an audit trail.[15]

Similar to the DoD 5015.2-STD standard, the European Commission's DLM Forum[16] developed the Model Requirements (MoReq®) in 2001 as a framework to guide the development of electronic record management systems. It evolved in 2008 to become MoReq2® and in 2011 it assumed its current form MoReq2010®. A key conceptual difference between MoReq2010® and its predecessors is the articulation of 'event histories' in lieu of 'audit trails'. While MoReq2010® acknowledges the need for audit trails to satisfy ISO 15489 requirements for "…complete and accurate representations of all transactions that occur in relation to a particular record…[it] adopts this approach but extends it by adopting the concept of an event history for each record from ISO 23081‑1:2006: Information and documentation — Records management processes —Metadata for records." Further, it infers the use of audit trails by noting that they "…may be conceptualised as a view of all events from the event histories of all entities across the whole MCRS [MoReq2010® compliant record system] (in timestamp order)." [17]

Finally from a recordkeeping point of view, ARMA International articulated in 2009 the need for audit trails in its *Generally Accepted Recordkeeping Principles.* The second principle, Integrity, calls for an acceptable audit trail, stating that these "…are essential in proving reliability of the recordkeeping actions of the organization…[and that]…acceptable audit and quality assurance processes should be in place."[18]

Archival Preservation and Audit Trails

In transitioning and transferring records from electronic recordkeeping systems to archival control and a preservation platform, archivists need to ensure that archival records are preserved in authentic form with intellectual control that describes the records according to standards that include contextual information sufficient to define the provenance, context, and structure of the records; it also means applying controls to any technological migrations or transformations in order to preserve authenticity, i.e. an audit trail.[19]

The Consultative Committee for Space Data Systems (CCSDS) developed the *Reference Model for an Open Archival Information System*, which has become commonly known as OAIS.[20] Adopted as an international standard in 2002 by ISO, the OAIS model accounts for actions by producers of information that is transferred to an archival preservation environment, where it is managed and eventually disseminated and utilized by consumers of information. Provenance information that is maintained in an OAIS provides an audit trail; it documents "…the origin or source of the Content Information, any changes that may have taken place since it was originated, and who has had custody of it since it was originated…[providing]…future users some assurance as to the likely reliability of the Content Information as it contributes to evidence supporting Authenticity."[21]

In 2007, the Center for Research Libraries (CRL) which administers the Trusted Repository Audit Checklist (TRAC), the developers of the Digital Repository Audit Method Based On Risk Assessment (DRAMBORA), and representatives of the Network of Expertise in long-term STORage (nestor) authored the "Core Requirements for Digital Archives" in order to "…[develop a] consensus on core criteria for digital preservation repositories, to guide further international efforts on auditing and certifying repositories." Among the ten requirements is one that addresses metadata management and audit trails: "Creates and maintains requisite metadata

about actions taken on digital objects during preservation as well as about the relevant production, access support, and usage process contexts before preservation."[22] TRAC and nestor's *Catalogue of Criteria for Trusted Digital Repositories*[23] identify directly the need for audit trails, whereas it is only inferred in DRAMBORA. [24]

The objective of TRAC, developed by OCLC's former Research Libraries Group and the U. S. National Archives and Records Administration, was to articulate criteria to identify digital repositories capable of reliably storing, migrating, and providing access to digital collections, with the criteria being derived from the OAIS model, thereby determining whether the repository is OAIS compliant or not. TRAC provides more than a dozen criteria that correspond to the use of audit trails.[25] OAIS and TRAC led to the development of two additional ISO standards: 16363 the audit and certification of trustworthy digital repositories; and 16919 which establishes requirements for bodies providing audit and certification of candidate trustworthy digital repositories.[26]

Initially a German Federal Ministry for Education and Research sponsored initiative, nestor since July of 2009 has acted as an independent network of partners comprised of digital preservationists, librarians, archivists, museum curators and other professionals who work together in the attempt to ensure long-term preservation and accessibility of digital sources.[27] The *Catalogue of Criteria for Trusted Digital Repositories* establishes criteria to evaluate digital repository trustworthiness from both technological and organizational points of view, similar to both the TRAC and DRAMBORA projects. Section B of the *Criteria Catalogue* is dedicated to object management. Item12.4 acknowledges that digital repositories, which utilize migration as a long-term preservation strategy, as a side-effect are ultimately changing the object to some extent. Therefore, it requires the digital repository to record adequate metadata to document all

the changes made by the digital repository to the digital objects. This includes not only the changes made to the digital object itself, but recording the people, systems and corresponding rights involved to document authenticity of the object, and to help ensure the technical preservation of the digital object. And it finally notes that the provenance/history/audit trail can be managed via metadata. [28]

Conclusion

National and international standards have been developed over the past two decades to identify system, process and metadata requirements for the management and preservation of electronic records. Among these requirements are those for audit trails. Maintaining audit trails are crucial for demonstrating the authenticity, reliability, integrity and usability of electronic records, not just at the point of appraisal and accessioning, but to provide provenance for electronic records from their point of creation, through their primary and active use by an individual or within an organization, and continuing throughout their archival life. This is especially necessary as permanent electronic records are transformed throughout their archival lives in order to remain accessible and understandable. Ultimately, if conducted methodically, it may actually provide electronic records with greater level of authenticity than their paper counterparts.

Additional Readings

Bantin, Philip C. “Developing a Strategy for Managing Electronic Records the Findings of the Indiana University Electronic Records Project.” *American Archivist*, 61 (Summer 1998): 328-364.

Bantin, Philip C. *Understanding Data and Information Systems for Recordkeeping*. London: Neal-Schuman Publishers, Inc., 2008

Cloonan, Michèle V. and Shelby Sanett. "Preservation Strategies for Electronic Records: Where We Are Now—Obliquity and Squint?" *American Archivist*, 65 (Summer 2002): 70-106.

University Archivists Group. "Standards for an Electronic Records Policy." Committee on Institutional Cooperation, 2001

Gable, Julie. "Everything You Wanted to Know About DoD 5015.2." *The Information Management Journal*, 36 (November/December, 2002): 32-38.

Glick, Kevin and Eliot Wilczek. "1.5 Requirements for Trustworthy Recordkeeping Systems and the Preservation of Electronic Records in a University Setting." *Fedora and the Preservation of University Records Project*. 2006. http://dl.tufts.edu/file_assets/tufts:UA069.004.001.00005

National Archives of Australia, "Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records." 2004. http://mayaarbinaginting.weebly.com/uploads/1/0/6/1/10612501/digital_recordkeeping.pdf

Rogers, Corinne. "Virtual Authenticity: Authenticity of Digital Records from Theory to Practice." PhD diss., The University of British Columbia, 2009.

Ross, Seamus and Andrew McHugh. "Preservation Pressure Points: Evaluating Diverse Evidence for Risk Management." http://www.repositoryaudit.eu/images/PreservationPressurePoints.pdf

[1] ARMA International, *Glossary of Records and Information Management Terms, 3rd edition* (Lenexa, KS: ARMA International, 2007), 3.

[2] Frederick J. Stielow, "Archival Theory and the Preservation of Electronic Media: Opportunities and Standards Below the Cutting Edge," *American Archivis*t 55 (Spring 1992): 334.

[3] Margaret Hedstrom, "Electronic Archives: Integrity and Access in the Network Environment," *American Archivist* 58 (Summer 1995): 315-316.

[4] Richard Pearce-Moses, *A Glossary of Archival and Records Terminology*, Society of American Archivists. Accessed June 4, 2015. http://www2.archivists.org/glossary/terms/p/provenance

[5] ISO, *ISO-154890-1Information and documentation – Records management – Part 1: General* (Geneva, Switzerland: 2001): 7

[6] Anne J. Gilliland-Swetland, "Testing Our Truths: Delineating the Parameters of the Authentic Archival Electronic Record," *American Archivist*, 65 (Fall/Winter 2002): 197-198

[7] *The InterPARES 2 Project Glossary*. Accessed June 11, 2015. http://www.interpares.org/ip2/display_file.cfm?doc=ip2_glossary.pdf&CFID=6629095&CFTOKEN=53559569

[8] Additional definitions include: "An electronic means of tracking interactions with records within an electronic system so that any access to the record within the electronic system can be documented as it occurs or afterward. May be used to identify unauthorized actions in relation to the records, e.g., modification, deletion, or addition." United States Government, Defense , U.S. Department of, "DoD 5015.2-ST: Design Criteria Standard for Electronic Records Management Software Applications," (Assistant Secretary of Defense for Command, Control, Communications and Intelligence, 2002): 8; "In a records and archives environment, a record showing the transactions within an information management system providing evidence of activities, such as who has

accessed a computer system and when, what operations he or she has performed during a given time and the resulting changes to records or information." Laura Millar, editor, *Training in Electronic Records Management: Glossary of Terms* (London: International Records Management Trust, 2009), 7; "In a traditional business system, a centralised log of all, or significant, system activity. An MCRS [MoReq2010® compliant records system] keeps a trail of its activities as a sequence of events, which may be viewed across the system as a whole, but are more commonly accessed as an event history for an individual entity." DLM Forum Foundation, *MoReq2010® Modular Requirements for Records Systems* (2010 & 2011): 198

[9] David Bearman and Ken Sochats, "Functional Requirements for Evidence in Recordkeeping: The Pittsburgh Project," (1996). Accessed June 11, 2015. http://www.archimuse.com/papers/nhprc/BACartic.html

[10] Luciana Duranti and Heather MacNeil, "The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project," *Archivaria* 42 (Fall 1996): 47-48.

[11] Terry A. Halvorsen, U.S. Department of Defense Office of the Chief Information Officer, *Memorandum: DoD Records Management Program* February 24, 2015. Accessed July 9, 2015. http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf

[12] John W. Carlin, "Baseline Requirements for Automated Record keeping," (November 18, 1998). Accessed August 6, 2015. http://www.archives.gov/records-mgmt/policy/automated-recordkeeping-requirements.html

[13] U.S. Department of Defense, "DoD 5015.02-STD Electronic Records Management Software Applications Design Criteria Standard," (April 25, 2007) 53-43 and 56. Accessed June 25, 2015. http://jitc.fhu.disa.mil/projects/rma/downloads/p50152stdapr07.pdf

[14] Luciana Duranti, "Introduction," *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project.* Accessed June 4, 2015. http://www.interpares.org/book/interpares_book_c_intro.pdf

[15] InterPARES Authenticity Task Force, "Appendix 2: Requirements for Assessing and Maintaining the Authenticity of Electronic Records," *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, (March 2002) 6-8. Accessed June 11, 2015. http://www.interpares.org/book/interpares_book_k_app02.pdf

[16] 'Données Lisibles par Machine' or machine-readable data

[17] DLM Forum Foundation, "MoReq2010®: Modular Requirements for Records Systems — Volume 1: Core Services & Plug-in Modules," (2011): 28 and 38. Additionally look to sections 2.2.8 Event Histories (37) and 3.2.2 Requirements for records management (51). Accessed June4, 2015. http://www.moreq.info/files/moreq2010_vol1_v1_1_en.pdf

[18] ARMA International, "ARMA International> Principle of Integrity" Accessed August 12, 2015. http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles/integrity

[19] International Council on Archives, "Guide for Managing Electronic Records from an Archival Perspective," (February 1997): 34

[20] Founded in 1982 by the major space agencies of the world, the CCSDS is a multi-national forum for the development of communications and data systems standards for spaceflight. Accessed August 12, 2015. http://public.ccsds.org/default.aspx.

[21] CCSDS, "Reference Model for an Open Archival Information System (OAIS)," (June 2012): 4-30. Accessed June 4, 2105. http://public.ccsds.org/publications/archive/650x0m2.pdf

[22] Center for Research Libraries, "Ten Principles | CRL," Accessed August 12, 2015. https://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/core-re

[23] nestor Working Group -Trusted Repositories Certification, "Catalogue of Criteria for Trusted Digital Repositories Version 1 (draft for public comment)," (Frankfurt, Germany: December 2006), http://files.d-nb.de/nestor/materialien/nestor_mat_08-eng.pdf and "Catalogue of Criteria for Trusted Digital Repositories – Version 2," (Frankfurt, Germany: November 2009), http://www.langzeitarchivierung.de/Subsites/nestor/SharedDocs/Downloads/materialien/nestor_mat_08_eng.pdf;jsessionid=390234DF257102531658BA817262C7E2.prod-worker2?__blob=publicationFile. Accessed August 13, 2015.

[24] The only recognition of audit trails in the DRAMBORA criteria is the following statement, "After completing the assessment, you will have two distinct outputs: 1. a risk register… 2. an audit report structured along the ten characteristics of digital preservation repositories…" Martin Donnelly, Perla Innocenti, Andrew McHugh, and Raivo Ruusalepp, "DRAMBORA interactive User Guide," (Glasgow, 2009): 6. Accessed August 5, 2015. http://www.dcc.ac.uk/sites/default/files/DRAMBORA_Interactive_Manual%5B1%5D.pdf

[25] Requirements: B1.3, B1.5, B2.3, B2.4, B2.11, B2.12, B.4.4, B6.3, B6.5, B6.6, B6.7, B6.8, B6.9, C1.2, C1.6, and C1.8 in OCLC and CRL's "Trustworthy Repositories Audit & Certification: Criteria and Checklist, Version 1.0" (February 2007): 22 – 46. Accessed August 6, 2015. https://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf

[26] Initially developed in 2011 as CCSDS's "Recommendation for Space Data System Practices, Audit and Certification of Trustworthy Digital Repositories CCSDS 652.0-M-1" (http://public.ccsds.org/publications/archive/652x0m1.pdf), it was adopted by ISO in 2012 as "ISO 16363 Space data and information transfer systems -- Audit and certification of trustworthy digital repositories" (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56510&commid=46612). Similarly, CCSDS's 2014 "Recommendation for Space Data System Practices Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories CCSDS 652.1-M-2" (http://public.ccsds.org/publications/archive/652x1m2.pdf) was adopted by ISO in 2014 as "ISO 16919 Space data and information transfer systems -- Requirements for bodies providing audit and certification of candidate trustworthy digital repositories" (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57950&commid=46612). Accessed August 12, 2015.

[27] nestor, "Welcome to nestor," Accessed August 6, 2015. http://www.langzeitarchivierung.de/Subsites/nestor/EN/Home/home_node.html;jsessionid=390234DF257102531658BA817262C7E2.prod-worker2

[28] nestor Working Group on Trusted Repositories Certification, "Catalogue of Criteria for Trusted Digital Repositories – Version 2," (Frankfurt, Germany: November 2009): 33. Accessed August 13, 2015. http://www.langzeitarchivierung.de/Subsites/nestor/SharedDocs/Downloads/materialien/nestor_mat_08_eng.pdf;jsessionid=390234DF257102531658BA817262C7E2.prod-worker2?__blob=publicationFile